AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A countermeasure method against attacks by differential analysis of current consumption in an electronic component [[using]] having a microprocessor and memory for executing a cryptographic algorithm having a secret key, comprising the following steps:

executing, by the microprocessor, a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means stored in the memory to deliver output data on the basis of input data, and

executing, by the microprocessor, another set of said critical instructions with other manipulating means stored in the memory that are derived from said first manipulating means by complementation of at least one of said input data and said output data, so that the output data and data derived from said output data are unpredictable.

2. (Previously Presented) A countermeasure method according to claim 1, wherein said first and said other manipulating means are selected for use on the basis of one-half probability statistical relationship.

3. (Previously Presented) A countermeasure method according to claim 2, wherein said algorithm comprises sixteen computation rounds, and wherein said

method comprises executing a first sequence and a second sequence, each of which is made up of at least the first three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means in at least the first round.

4. (Previously Presented) A countermeasure method according to claim 3, wherein each of the first and second sequences is made up of the first three rounds.

5. (Previously Presented) A countermeasure method according to claim 3, wherein said other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data.

6. (Previously Presented) A countermeasure method according to claim 2, wherein said algorithm comprises sixteen computation rounds, and wherein said method comprises executing a first sequence and a second sequence, each of which is made up of at least the last three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means.

7. (Previously Presented) A countermeasure method according to claim 6, wherein each of the first and second sequences is made up of the last three rounds, and wherein the other manipulating means used in the second sequence comprise second manipulating means and a third manipulating means.

8. (Previously Presented) A countermeasure method according to claim 7, wherein said second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said second manipulating means are used in the second sequence for the fourteenth round.

9. (Previously Presented) A countermeasure method according to claim 8, wherein said third manipulating means are such that, for the complement of the input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said third manipulating means are used in the second sequence for the fifteenth round and the sixteenth round.

10. (Previously Presented) A countermeasure method according to claim 1 wherein said manipulating means are tables of constants.

Claims 11-12. (Canceled)

13. (Previously Presented) An electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm, comprising:

a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data;

a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means; and

means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced thereby is unpredictable.

14. (Previously Presented) The electronic component of claim 13 wherein said manipulating means comprise tables of constants.

15. (Previously Presented) The electronic component of claim 13 wherein said different manipulating means respectively produce sets of output data that are complementary to one another.

16. (Previously Presented) The electronic component of claim 13, wherein said component is a smart card.